AMENDMENTS TO THE SPECIFICATION

Please replace the title with the following amended title:

AUTOMATED DIAGNOSIS FOR ~~ELECTRONIC SYSTEMS~~ COMPUTER NETWORKS

Please replace the paragraph on page 16, lines 8-25 with the following amended paragraph:

The verification process is described as follows. In an example, verification is performed to check that the ranked potential causes are reasonable and not just coincidental policy changes and not related to the problem described in the input process. Security and reliability vulnerabilities are determined by using the EDD 210 and HVD 212 as described in U.S. ~~patent application, serial no. N/A~~ Patent No. 7,237,266, entitled "Electronic ~~Profile and Policy~~ Vulnerability and Reliability Assessment," and incorporated by this reference herein. In a preferred embodiment the HVD 212 is configured with system elements at a top level (i.e., general levels) and branches down to a multiplicity of specific security vulnerabilities ~~as the~~ at the bottom level (i.e., more specific levels). One of the main problem parameters is the element or elements in which the problem occurred or was noted, and this provides a starting point at the top level of the HVD 212 for verification. In an example, the potential causes which need to be verified, correspond to at least a partial policy configuration that provides information for the middle level of the HVD 212 which can be augmented by additional policy configuration information obtained by the policy interpreter module 316 if necessary to make progress down through the database. The problem itself is a set of symptoms or "observables" associated with one or more specific security vulnerabilities located at the bottom levels of the HVD 212.

Please replace the paragraph on page 16, line 26 through page 17, line 2 with the following amended paragraph:

In a preferred embodiment, the verification process is performed by the verifier module 306 utilizing the processes disclosed in U.S. ~~patent application, serial no. N/A~~ Patent No. 7,237,266, entitled "Electronic ~~Profile and Policy~~ Vulnerability and Reliability Assessment," to

proceed down through the HVD 212 for each potential cause. Each potential cause, together with additional policy information, if needed, provides the policy information that controls the branching downward through the levels of the HVD 212, and thus forms a path from the top level starting point to some point on a bottom level. If this path reaches a bottom most destination matching or approximately matching the identified problem, then the respective potential cause is considered verified. Otherwise, the potential cause is not verified.

Please replace the paragraph on page 17, lines 3-9 with the following replacement paragraph:

In a preferred embodiment, the policy interpreter module 316 ~~provide~~ provides aspects and details of the overall system's policy for the system under review to the verifier module 306 as needed in the verification process, interfacing with the overall system's policy management capability to do so. In an alternative embodiment, the policy interpreter module 316 utilizes a complete set of policy information via the described input parser/filter input process as described in U.S. ~~patent application~~ Patent No. 7,237,266, entitled "Electronic ~~Profile and Policy~~ Vulnerability and Reliability ~~Assessment,"~~ Assessment."

Please replace the paragraph on page 19, line 30 through page 20, lines 19 with the following replacement paragraph:

Referring to FIG. 5B, at 516, the ranked potential causes are tested utilizing database cycling in order to verify that they may be actual causes of the problem. In a preferred embodiment, the potential causes are verified by utilizing information contained in the EDD 210 and HVD 212 and a process as described in U.S. ~~patent application, serial no. N/A~~ Patent No. 7,237,266, entitled "Electronic ~~Profile and Policy~~ Vulnerability and Reliability Assessment." At 518, the distances are calculated. At 520, a determination is made by a distance estimator module as to whether or not threshold levels set by the user or administrator are violated. If yes, at 522, the rankings in violation are discarded or decreased. In some embodiments, potential causes can be discarded using a configurable distance threshold set by the user such that any possible causes with distances that exceed this threshold value are deemed exceedingly unlikely to be actual causes, and therefore can be eliminated and subsequently ignored. In this example,

the verification process verifies only the first and second potential causes. The third potential cause is discarded since it is determined to not be able to cause any vulnerability corresponding to the noted problem, and thus is not verified. The second change results in a very large verification distance, which subtracts greatly from its ranking, although it is not large enough to cause it to be discarded (i.e., its distance does not exceed the configurable threshold). The first change has a very small verification distance, which negligibly subtracts from its high ranking. If the threshold is not violated for one or more potential causes, at 524, a finalized ordered list of likely causes is prepared. For example, utilizing information from the EDD 210, preliminary rankings are adjusted to form the final rankings (e.g., final distances).